Kryptografie včera, dnes a zítra

Jan Paseka

O čem to dnes bude

- Úvod do problematiky, motivace
- Historie
- Symetrické šifrování
- Asymetrické šifrování
- Digitální podpis
- Šifrovací algoritmy
- PGP, kvantová kryptografie

Základní pojmy (1)

- Kryptologie

  věda zabývající se šiframi

- Kryptografie

  část kryptologie zabývající se převedením srozumitelné zprávy do nesrozumitelné podoby a zpět (šifrování a dešifrování textu)

- Kryptoanalýza

  část kryptologie zabývající se odhalením klíče, čili umožněním čtení zašifrované zprávy

Základní pojmy (2)

- Šifrování (encryption)

  proces, při kterém převedeme podle určených pravidel otevřený text na šifrový text (cipher text)

- Dešifrování (decryption)

  opačný proces k šifrování

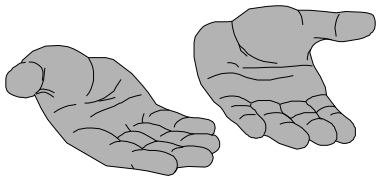
- Klíč

  posloupnost, může být rozdílný pro šifrování a dešifrování

- Útok na šifru, lámání šifry

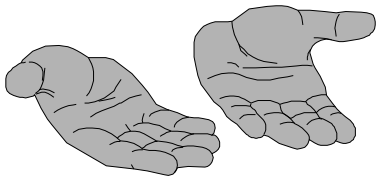
  zkoušení všech možných klíčů

Proč šifrovat?



- Bankovnictví
- Multimédia – DVD, CD, SAT TV
- Firemní korespondence, Obyčejný mail = pohlednice
- odchozí dráty, routery, SMTP servery, POP3 server
- konkurence, váš obchodní partner, znuděný hacker, admin, který dostal výpověď, někdo, koho jste naštval
- vyzrazení dat, modifikace dat
- Pokud je tajnost zprávy závislá na utajení algoritmu šifrování, je to VŽDY špatně
- Současné algoritmy šifrování jsou obecně známé a tajnost zprávy závisí pouze na tajnosti klíče

Proč šifrovat?



- **Kryptologie, která byla dříve výsadou tajných služeb, armád a diplomacie, se stává během posledních deseti let věcí veřejnou a současně i výnosným obchodem. Zahajuje svoje masové tažení za všemi uživateli výpočetní techniky. Pojmy jako státní informační systém, e-business, e-commerce, e-obchodování, elektronický notář, kvalifikovaný certifikát, ochrana osobních dat a další se stanou samozřejmou součástí našeho jazyka a jejich realizace je možná právě díky kvalitním kryptografickým produktům a právnímu zajištění.**

Nejstarší šifry, historie

- **Skytála (transpoziční šifry)**

  Před 2500 lety používala vláda ve Spartě následující metodu pro přenos tajné zprávy pro své generály: odesilatel a příjemce museli mít oba tzv. skytálu:

  byly to dva válce o přesně stejném průměru.

  Odesilatel navinul úzkou pergamenovou pásku spirálovitě okolo své skytály a napsal pak podle délky svou zprávu na pásku. Po odmotání pásky mohla zprávu číst jen ta osoba, která měla skytálu stejného rozměru --

  doufejme, že to byl pouze příjemce .

Nejstarší šifry, historie

- **Caesarova šifra (posouvací šifry)**

  římský vojevůdce a státník Gaius Julius Caesar (100-44 př. n. l.).

  Existují také [Caesarovy dopisy] Cicerovi a známým o věcech, v kterých psal tajným písmem, pokud něco muselo být důvěrně sděleno. Tzn. změnil pořadí písmen tak, že nešlo zjistit jediné slovo. Pokud někdo chtěl toto rozluštit apoznat obsah, musel dosadit čtvrté písmeno abecedy, tedy D, za A, a podobně toto provést se zbývajícími písmeny.

  My můžeme ale posunout abecedu o libovolný možný počet míst. Protože se naše abeceda sestává z 26 písmen, existuje právě 26 takových šifrování - mluvíme o posouvacích neboli aditivních šifrách.

Nejstarší šifry, historie

- **počátek dvacátého století století - prudký rozvoj, telegraf**

  V současnosti leží hlavní úloha kryptografie v utajování elektronické komunikace. Krátce poté, co Samuel F. B. Morse v roce 1845 veřejně předvedl telegraf, objevily se obavy před vyzrazením posílaných zpráv.

  Co se stane, kdyby někdo zcizil telegrafní pásku? Co zabrání nepoctivému telegrafnímu úředníkovi ve zkopírování zprávy a jejímu případnému vyzrazení?

  Odpověd spočívala v kódování tajným kódem, který nemohl rozluštit nikdo jiný než oprávěný příjemce. Význam kryptografie dále stoupl s objevem radiové komunikace a s jejím použitím ve válkách. Bez použití kryptografie by mohl nepřítel velmi snadno zachytit zprávy, vysílané z fronty nebo na frontu.

Nejstarší šifry, historie

- **počátek dvacátého století století - prudký rozvoj, telegraf**

  Vstup USA do I. světové války byl důsledkem vyluštění obsahu šifrového telegramu -- dnes známého jako tzv. Zimmermannův telegram, kde německý ministr zahraničí Zimmermann v telegramu mexické vládě vyzývá Mexiko k válce proti USA. Slibuje v ní mexické straně podporu a územní zisk.

  Britové telegram zachytili, rozluštili jej a předali USA. Poté, co se prezident Wilson s obsahem telegramu seznámil, svolává Kongres. Ten 2.4.1917 schvaluje vstup USA do války proti Německu. Tento akt rozhodujícím způsobem změnil poměr sil na evropském bojišti.

Nejstarší šifry, historie

- **Vernamova šifra**

- **Je to asi jediná šifrovací metoda, jejíž bezpečnost je matematicky dokazatelná. Její princip spočívá v tom, že se zpráva zakóduje pomocí stejně dlouhé náhodné posloupnosti (klíče), čímž získá charakter zcela náhodného sledu znaků. Takový klíč může být pochopitelně použit pouze jednou (proto se této metodě v angličtině říká také one time pad) a musí být skutečně náhodný a nekorelovaný. Bez znalosti klíče nelze zprávu rozluštit. Jinými slovy, pravděpodobnosti všech možných výsledků jsou stejné. Neoprávněný luštitel má stejnou šanci dostat Shakespearovy sonety jako třeba daňové zákony. Opakované použití klíče nebo jeho části, či jakákoli pravidelnost v něm mohou dát luštitelům určitou šanci.**

Nejstarší šifry, historie

Vernamova šifra

- **Jak šifrování a dešifrování probíhá, ukazuje následující jednoduchý příklad. Používáme-li např. abecedu o 26 znacích, potřebujeme jako klíč sekvenci náhodných čísel z intervalu 0 až 25 (odesílatel i příjemce musí mít pochopitelně stejný klíč). Při šifrování se prostě posuneme v abecedě o patřičný počet míst (daný odpovídající hodnotou klíče) vpřed, při dešifrování vzad.**
- **V případě binárně kódované zprávy je situace ještě jednodušší. Klíč má podobu náhodné posloupnosti nul a jedniček (stejně dlouhé, jako je zpráva), kterou můžeme získat třeba házením mincí. Při šifrování i dešifrování se bity zprávy a klíče jednoduše sečtou modulo 2 (operace XOR):**

Zpráva	Klíč	Šifra	
1	1	0	11→ 0
1	0	1	
1	1	0	10→ 1
0	0	0	
0	0	0	01→ 1
0	1	1	
0	1	1	00→ 0

Nejstarší šifry, historie

- **do konce 50.let mnoho šifrovacích strojů (Enigma, Navajos)**

  Tento stroj způsobil zavedení počítačů do kryptografie a je základním kamenem pro pochopení způsobu práce moderních šifrovacích programů.

  Mezi velmi úspěšné kryptografické stroje použité během II. sv. války se dají zařadit tzv. Code-talkers (film Windtalkers)— příslušníci indianského kmene Navajo. Často používané výrazy měly přímo definovaný kód v navajštině, u ostatních slov bylo jejich každé písmeno při šifrovánínahrazeno anglickým slovem (z pevně definované sady), na toto písmeno začínajícím a to bylo posléze převedeno do Navajštiny (buď jako ekvivalent nebo opis původně v tomto jazyce neexistujícího slova). Díky pečlivě volenému kódovaní slov nebylo toto šifrování během války prolomeno ani přesto, že Japonci mohli využít příslušníka kmene Navajo pro překlad zachycených termínů

Nejstarší šifry, historie

Enigma způsobila zavedení počítačů do kryptografie a je základním kamenem pro pochopení způsobu práce moderních šifrovacích programů. Enigmu vyvinul na počátku 20. století Arthur Scherbius a začala se používat v dobách 2. světové války.

Šifrovací stroj Enigma se skládal z baterie, tlačítka pro každé písmeno abecedy, žárovky pro každé písmeno abecedy tzv. „lampboardu“ a ze série otočných disků, takzvaných rotorů. Před klávesnicí Enigmy leží ještě deska zvaná „plugboard“, což je ve skutečnosti 26 konektorů, pomocí kterých se mohou spojovat jednotlivá písmena, např. C na P apod.

Nejstarší šifry, historie

Princip Enigmy odpovídal dětské hračce: po zmáčknutí tlačítka se rozsvítilo nějaké světýlko. Když se pootočily rotory, změnilo se přiřazení mezi tlačítky a světýlky. Rotory byly rozhodující zařízení pro šifrovací schopnosti stroje. Každý rotor se tak trochu podobal sendviči s 52 kontakty na každé straně. Uvnitř rotoru bylo 52 drátků, z nichž každý spojoval dva kontakty na dvou stranách rotoru. Drátky ovšem nespojovaly odpovídající si kontakty na obou stranách, propojovaly je v rozházeném pořadí, takže například kontakt č. 1 na levé vnitřní straně rotoru byl spojen s kontaktem č. 15 na pravé vnitřní straně rotoru a podobně.

Nejstarší šifry, historie

Enigma používala tři rotory za sebou. Na konci řady rotorů byl reflektor, který poslal elektrický signál zpět ke druhému průchodu strojem. (Na konci války používal systém se čtyřmi rotory.) Polovina z 52 kontaktů byla napojena na tlačítka a baterii, druhá polovina byla připojena k žárovkám. Stisknutím každého tlačítka způsobilo uzavření obvodu a rozsvítila se určitá žárovka. Která žárovka se však rozsvítí, to záleželo na poloze všech tří rotorů a reflektoru. Při šifrování nebo dešifrování zprávy nastavil šifér rotory do určité výchozí pozice - to byl klíč. Pro každé písmeno zprávy teď zmáčkl tlačítko, zapsal, které písmeno se rozsvítilo a pootočil rotory.

Nejstarší šifry, historie

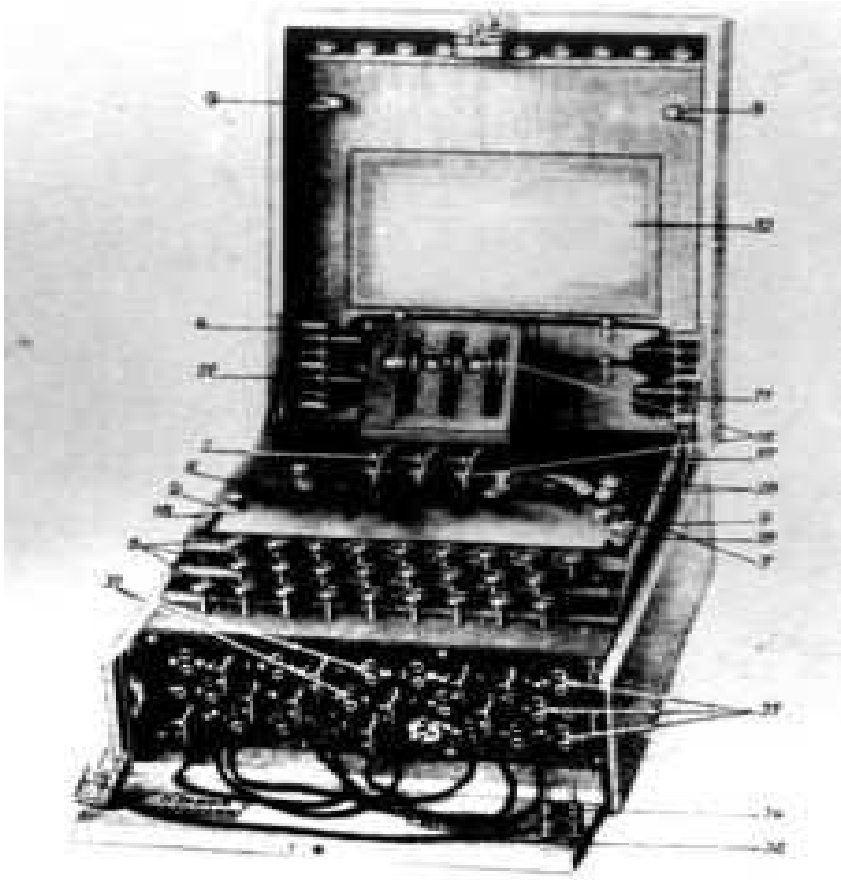
Protože se rotory pootočily po každém znaku, bylo stejné písmeno vstupního textu obvykle zašifrováno vždy jako dvě jiná.

Enigma tedy byla substituční stroj s jinou substitucí pro každý znak zprávy - tomuto druhu šifer se říká polyalfabetické šifry.

Namísto mezery se používalo písmeno Z, čísla se rozepisovala. Dešifrování zprávy bez znalosti počáteční polohy rotorů bylo (v té době) velmi obtížné.

Nejstarší šifry, historie

- **Obrázek Enigmy**



Nejstarší šifry, historie

- **50.-60. léta rozvoj počítačů, kryptografie pro veřejnost (banky)**

  Tato epocha je charakteristická 2 pracemi od Claude Elwood Shannona. V časopise Bell Systém Technical Journal v roce 1948 a 1949 otiskuje články "Matematická teorie sdělování" a "Sdělovací teorie tajných systémů".

  Prvý z článků dal vznik teorii informací, druhý článek pojednával o kryptologii v termínech informační teorie. Pojetí nadbytečnosti (redundancy) je hlavním termínem, který Shannon zavedl.

Nejstarší šifry, historie

- **1973 - požadavky na algoritmus na ochranu neutajovaných dat**

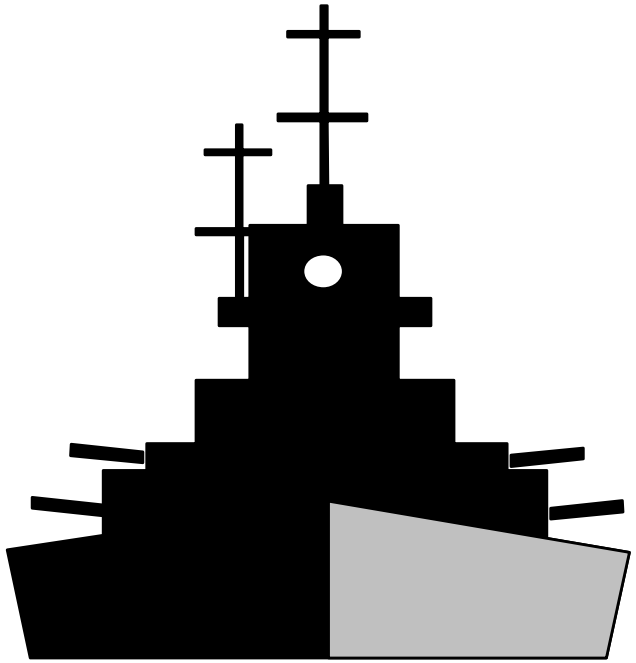
- **DES - Data Encryption Standard**

  Tento algoritmus byl vyvinut firmou IBM a v roce 1977 se stal veřejným standard pro ochranu informací, nikoliv však pro ochranu informací utajovaných. DES nešifruje písmena, nýbrž symboly 0 a 1, a to 64 naráz (v případě, že používáme DES k zašifrování obyčejného textu, musí být písmena nejdřív přeložena do řetězce bitů. Vývoj DES navazuje na vývoj šifrovacího algoritmu Lucifer od Thomase Watsona. Aktivní délka klíče je 56 bitů, hlavní prvky, které chrání šifrový text před útoky analytiků, jsou tzv. S-boxy. V roce 1976 byla uspořádána NBS (Národní úřad pro standardizaci) dvoudenní konference k diskuzi o DES.

- **množství šifer (symetrické i asymetrické), PGP**

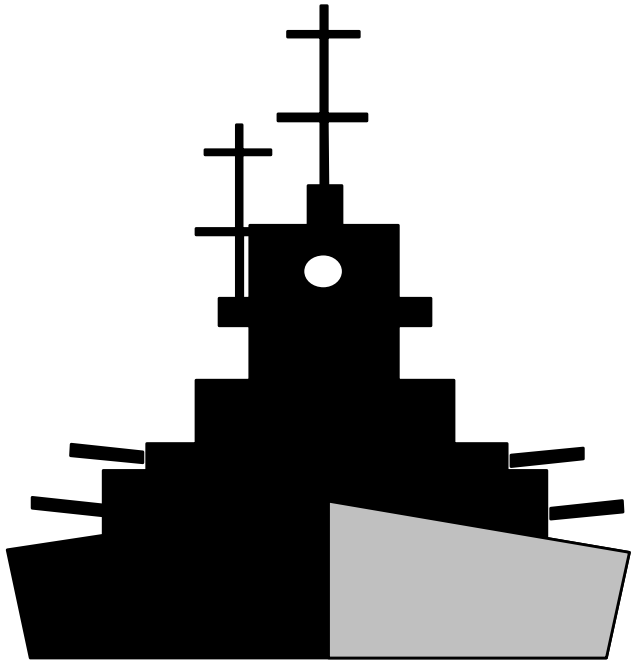
Export šifer

- Spojené státy považují šifrovací technologie za druh zbraně, a zbraně se samozřejmě neexportují jen tak ledaskam.



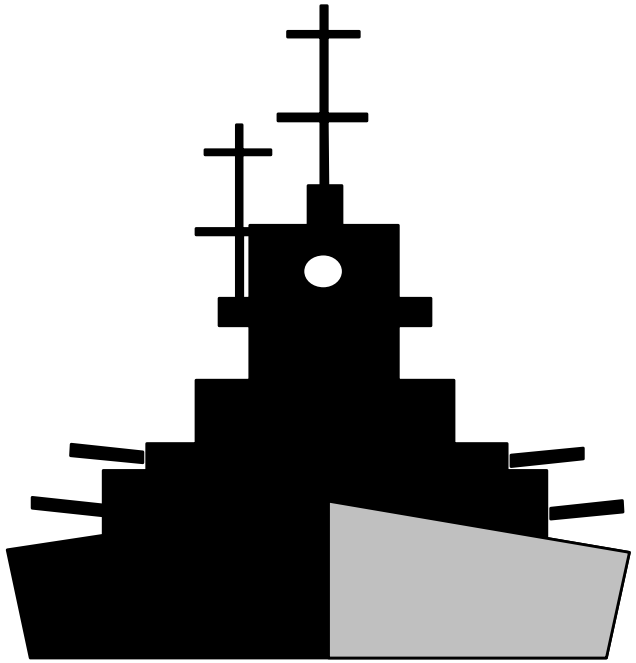
Export šifer

- I když se to na první pohled může zdát trochu nelogické, je koneckonců pravda, že rozluštění japonských šifer výrazně ovlivnilo průběh druhé světové války, takže i k tomu mají i pádný důvod.



Export šifer

- USA si ale zároveň uvědomují, že používání těchto technologií bude mít v blízké budoucnosti zásadní význam pro rozvoj elektronického obchodu a pravděpodobně i veškerého ostatního podnikání.



Export šifer

- **Zlomové roky 1999--2000**

- Již se neobjevují slabé šifrové systémy, které ještě v polovině 90. let byly předkládány veřejnosti jako bezpečné (např. Crypt, Rot13, SuperKey, N-Code).

- V produktech Microsoftu (Word, Excel), Lotusu, WordPerfectu se však stále používají nekvalitní šifrové systémy, které lze lehce rozbít. Postupně je Microsoft sice nahrazuje za kvalitní šifru, ale z důvodu vývozních omezení je oslabuje úpravou klíče na délku pouhých 40 bitů.

- Takto úmyslně upraveným algoritmům se říká slabá **kryptografie**. Mimo území USA a Kanady se tak stále v těchto produktech nacházejí slabé šifrové produkty.

Export šifer

- **Zlomové roky 1999--2000**

- Toto je ovšem výhodná situace pro evropské komerční firmy, které se snaží obsadit evropský trh svými produkty. Americké velké firmy se snaží donutit vládu USA k omezení vývozních restrikcí, ale ta neustupuje.

- Komerční produkty vybavené kvalitními symetrickými algoritmy (např. 3DES, CAST, RC4, Twofish) a asymetrickými algoritmy (RSA, algoritmy na bázi diskrétního algoritmu, algoritmy na bázi eliptických křivek) se začínají vyrábět a vyvážet nejen v Německu, Francii, Anglii, Finsku, ale i u nás.

- Česká firma Decros úspěšně vyváží své produkty nejen do Evropy, ale i do Asie. Květen 1999 je pro Českou republiku určitým ohodnocením naší vyspělosti v této oblasti. Výbor IACR v roce 1997 rozhodl, že konference Eurocrypt 1999 se bude konat v Praze.

Export šifer

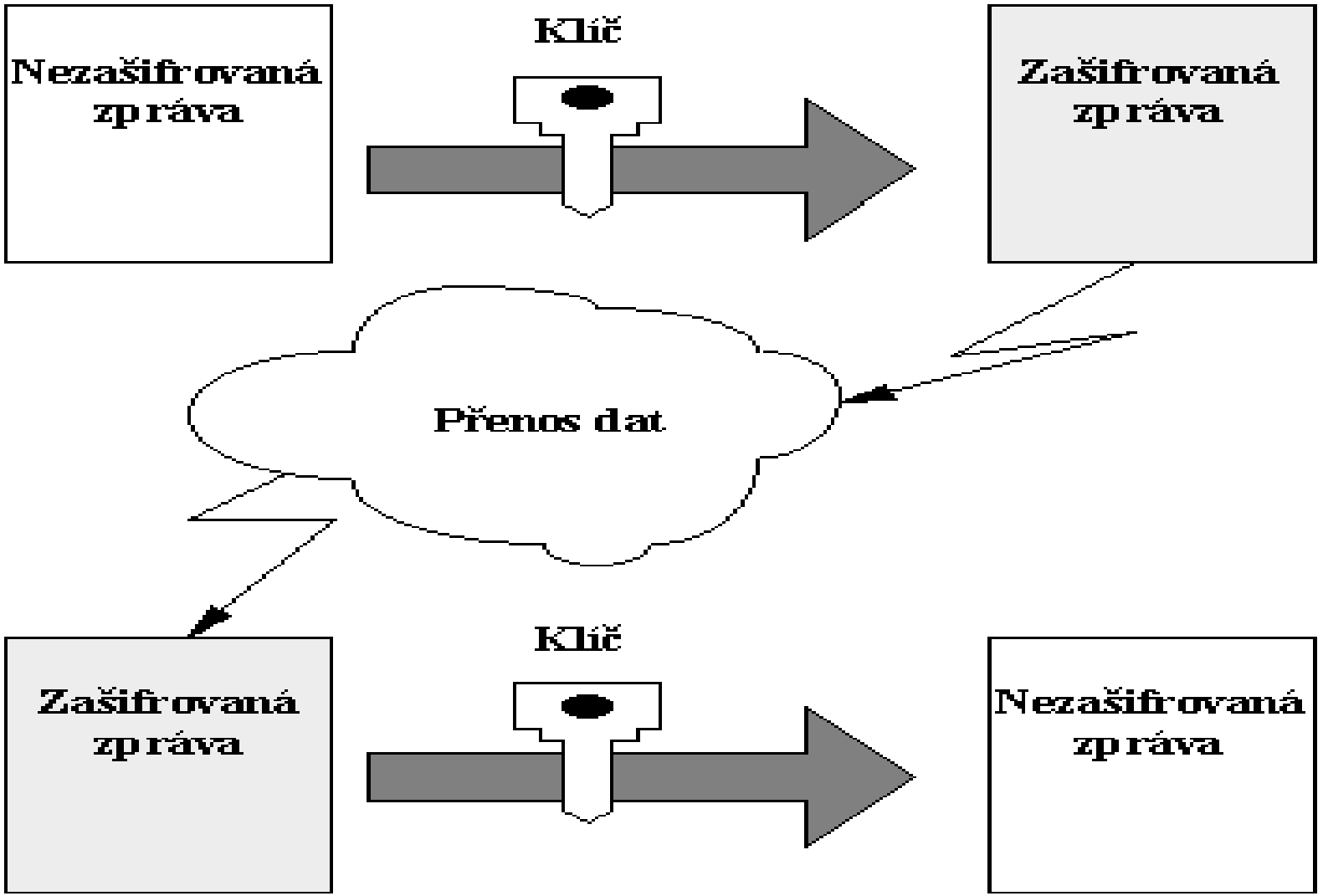
- **Zlomové roky 1999--2000**

- V létě 1999 německá vláda vydává prohlášení, ve kterém jasně proklamuje, že na dobu dvou let ruší všechny restrikce v používání silné **kryptografie** a dává celému světu najevo, že chce zaujmout rozhodující pozici v evropském trhu s kryptografií.

- Tlak amerických firem, které přicházejí o miliony dolarů, nakonec slaví úspěch. V listopadu 1999 dochází k prvnímu uvolnění vývozních restrikcí a další uvolnění následuje v lednu 2000. S konečnou platností je tak uvolněn **export** šifrovacích algoritmů ze Spojených států (včetně zdrojových textů).

- V lednu 2000 byl také zahájen 3 letý projekt NESSIE (New European Schemes for Signature, Integrity, and Encryption) programu IST Evropské komise. Jednotlivé moduly budou vytvářeny na základě veřejných návrhů a rovněž tak vyhodnocení těchto návrhů proběhne otevřenou a transparentní cestou.

Symetrické šifrování



Symetrické šifrování

- jeden klíč pro šifrování i dešifrování
- DES, 3DES, CAST, IDEA, Blowfish
- Výhody:

  rychlost

  hodí se pro data, která nikam nejdou (harddisk)
- Nevýhody:

  předání klíče

  počet klíčů (10000 členů = 50 milionů klíčů, 5 miliard lidí = 12 500 000 000 000 000 000 klíčů)

DES, 3DES

- Data Encryption Standard
- 1975, IBM
- NSA srazila klíč ze 128 na 56
- není moc bezpečný
- spec. stroj na zlomení DESu průměrně 3,5 hod v ceně
  cca. 1 mil. USD
- 3DES protáhne jedna data algoritmem třikrát - zašifrování nyní probíhá takto: zpráva se zašifruje pomocí algoritmu DES a klíče K1, odšifruje se pomocí klíče K2 a opět se zašifruje pomocí klíče K3 (resp. v jiné verzi klíčem K1). Délka klíče se tak vlastně 3x (resp.2x) prodloužila a toto řešení se tímto stalo odolné proti útoku hrubou silou.

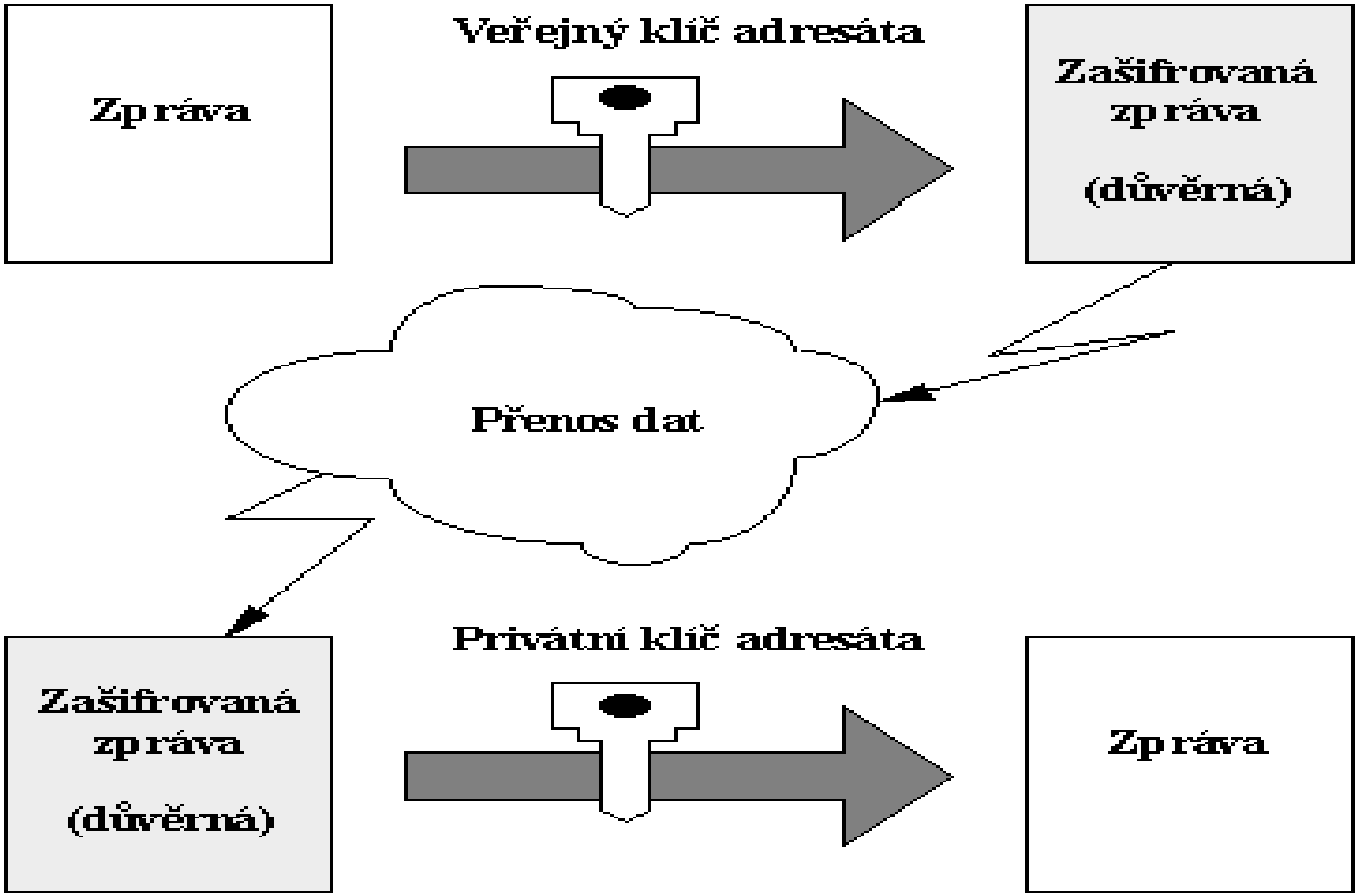
IDEA

- International Data Encryption Algorithm
- 1990, Xuejia Lai a James Massey
- Švýcarsko
- klíč 128 bitů
- implementována v rámci SSL
- není známo, že by byla rozluštěna metodou hrubé síly

AES

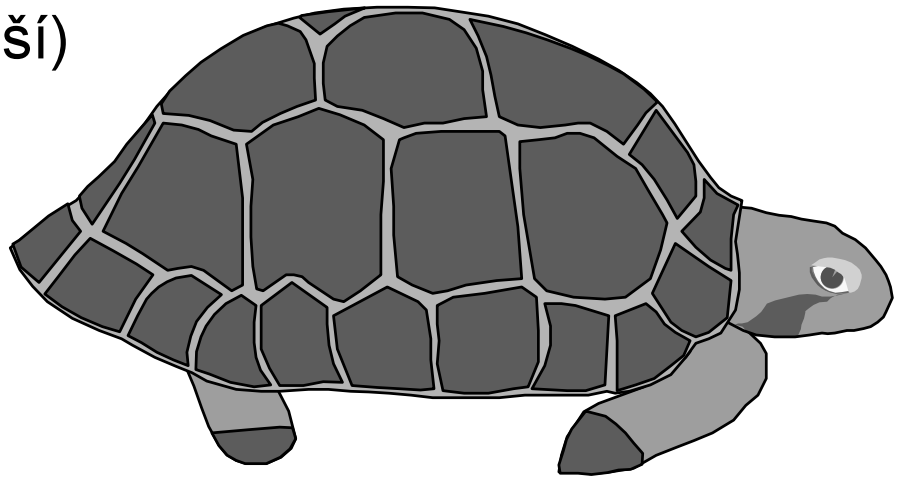
- V roce 1997 NIST vypisuje veřejnou soutěž na vytvoření nového komerčního standardu pro symetrické šifrování.
- Novým standardem se stal AES (Advanced Encryption Standard). AES má být 128bitová bloková šifra, musí podporovat klíče délky 128, 192 a 256 bitů. Je určen pro všechny typy aplikací a nasazení (klasický software pro PC, terminály pro elektronickou komerci, čipové karty).
- Algoritmus není patentován a vítěz dostává odměnu "zlatý vavřín kryptologie".

Asymetrické šifrování

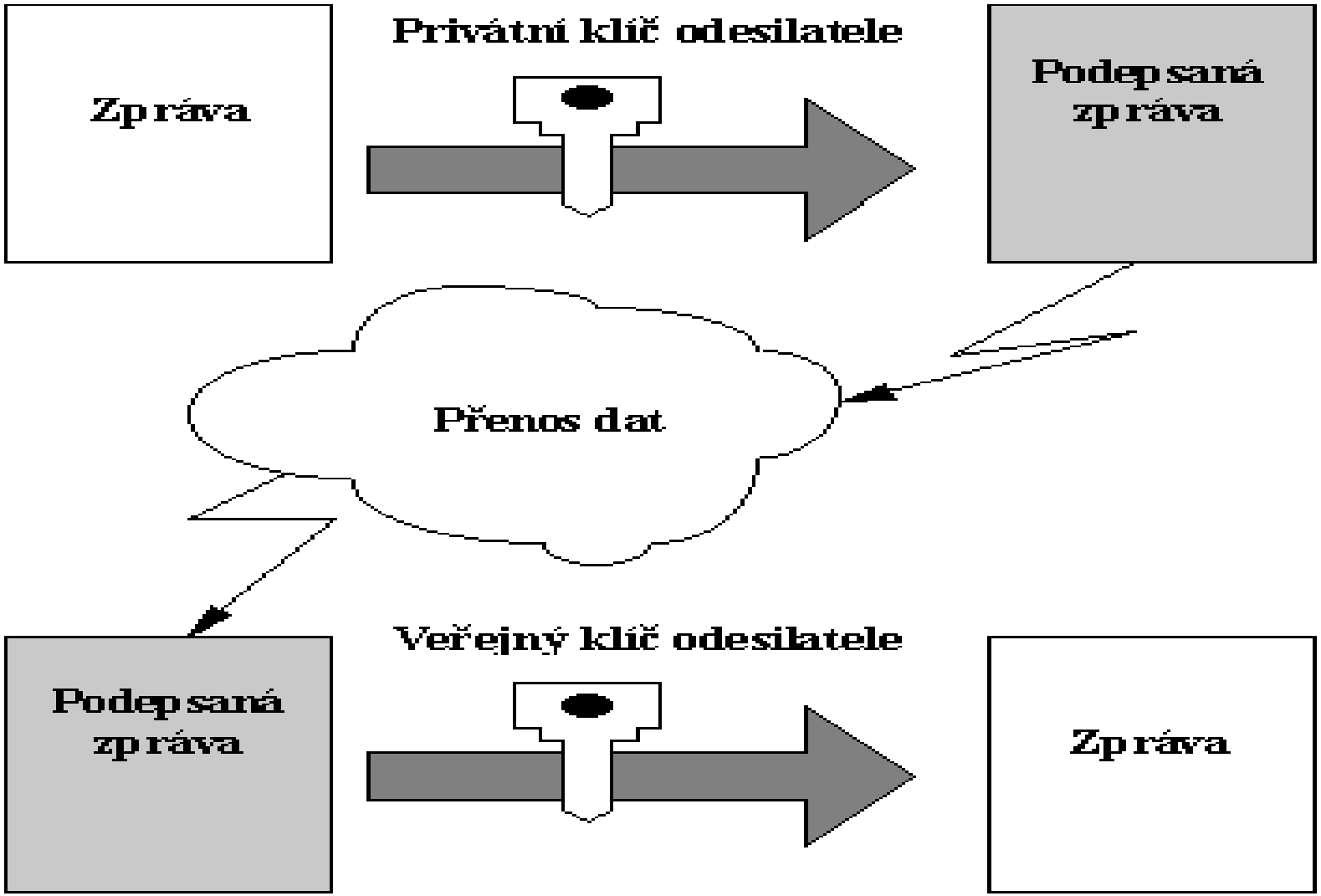


Asymetrické šifrování

- veřejný klíč + privátní klíč
- RSA, Diffie-Hellman, DSS
- Výhody:
  - odpadá předávání klíčů
  - menší počet klíčů
- Nevýhody:
  - „pomalost“ (asi 1000x pomalejší)



Digitální podpis



Digitální podpis

- *autenticita*

  podpis přesvědčí adresáta, že jste dokument skutečně podepsal.

- *nezfalšovatelnost*

  nikdo jiný váš podpis neumí napodobit.

- *jednorázovost použití*

  podpis nelze vzít a přenést na jiný dokument.

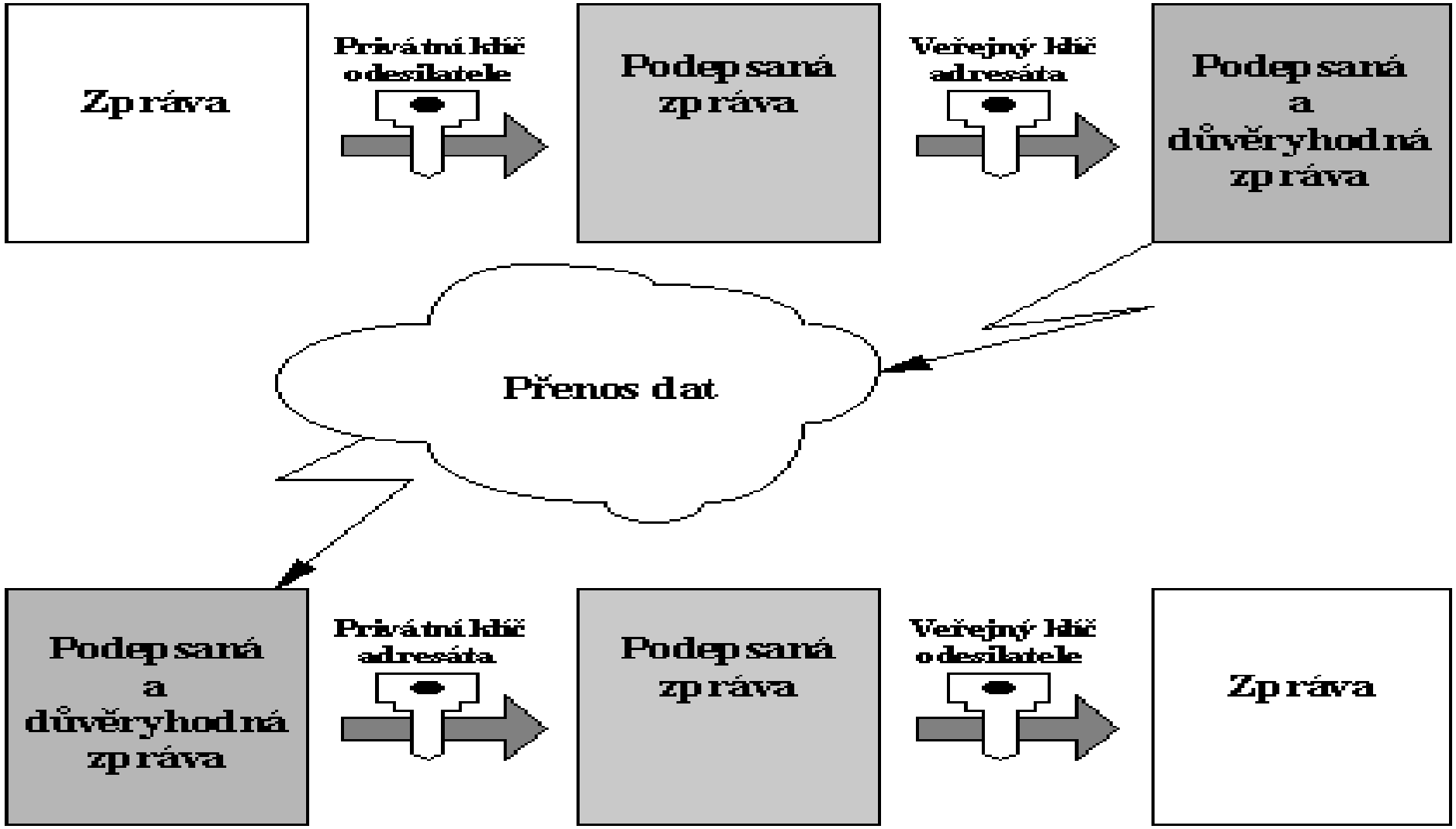
- *nezměnitelnost dokumentu*

  po podpisu už nelze provádět v textu žádné změny.

- *nepopiratelnost*

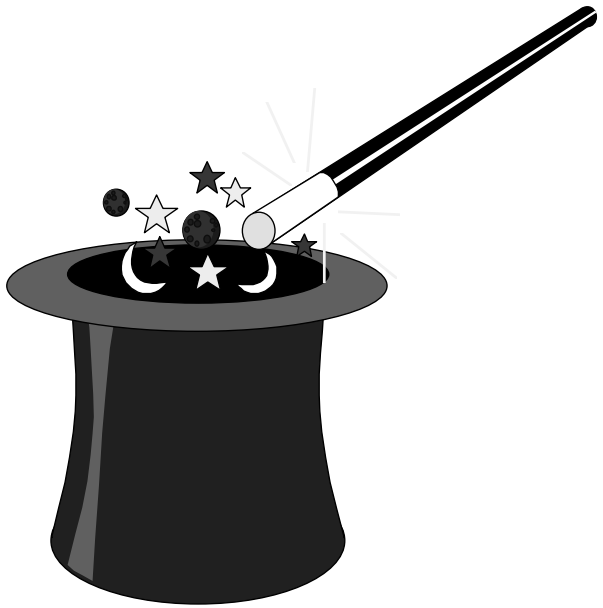
  nemůžete prohlásit, že jste dokument nepodepsal, když je vámi podepsaný

Digitální podpis

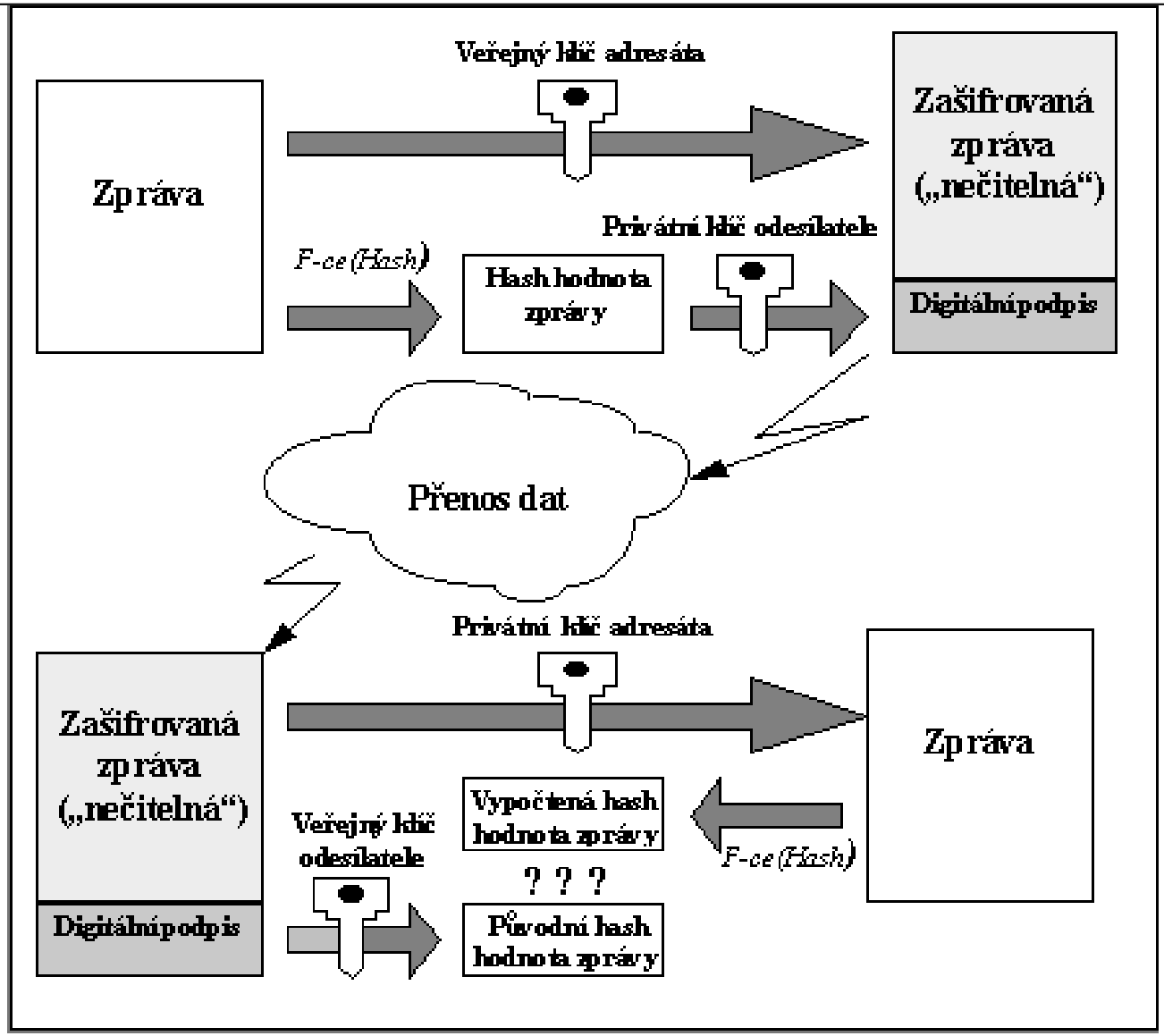


Hashovací funkce

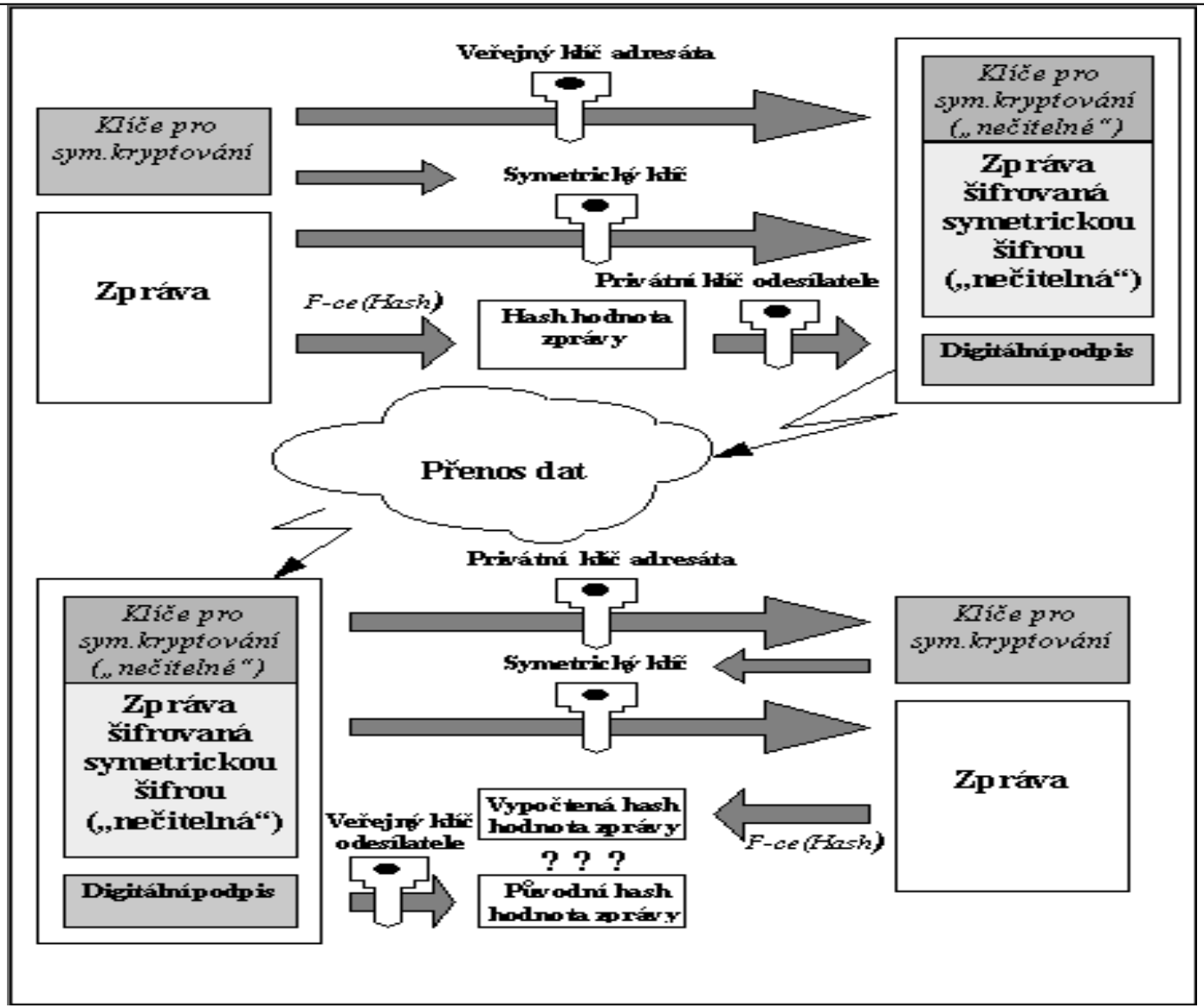
- funkce, která vyrobí vzorek jakéhokoli souboru (textu)
- výstupem je **vzorek** (hash, figerprint, otisk) o pevné délce, závislý na všech bitech původního souboru (textu)
- MD5 – Message Digest Algorithm 5
- SHA-1 – Secure Hash Algorithm 1



Praxe (1)

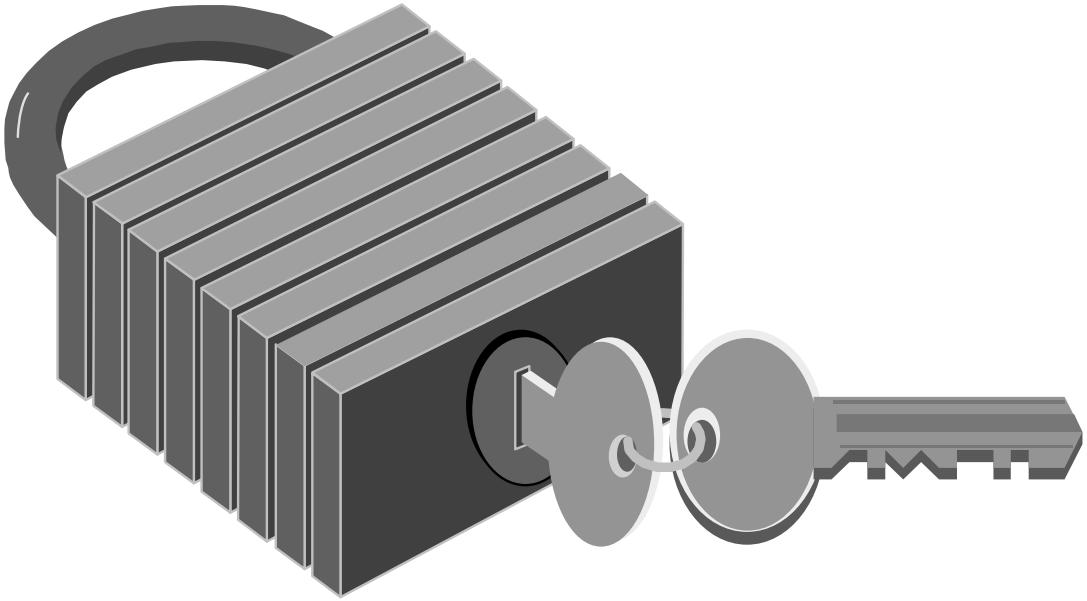

Veřejný klíč adresáta
Zpráva
Zašifrovaná zpráva („nečitelná“)
Privátní klíč odesílatele
F-ce (Hash)
Hash hodnota zprávy
Digitální podpis
Přenos dat
Privátní klíč adresáta
Zašifrovaná zpráva („nečitelná“)
Zpráva
Vypočtená hash hodnota zprávy
Veřejný klíč odesílatele
F-ce (Hash)
? ? ?
Digitální podpis
Původní hash hodnota zprávy

Praxe (2)


Veřejný klíč adresáta
Klíče pro sym.kryptování
Symetrický klíč
Zpráva
Privátní klíč odesílatele
F-ce (Hash)
Hash hodnota zprávy
Klíče pro sym.kryptování („nečitelné")
Zpráva šifrovaná symetrickou šifrou („nečitelná")
Digitální podpis
Přenos dat
Privátní klíč adresáta
Klíče pro sym.kryptování
Symetrický klíč
Klíče pro sym.kryptování („nečitelné")
Zpráva šifrovaná symetrickou šifrou („nečitelná")
Digitální podpis
Zpráva
Veřejný klíč odesílatele
Vypočtená hash hodnota zprávy
? ? ?
Původní hash hodnota zprávy
F-ce (Hash)

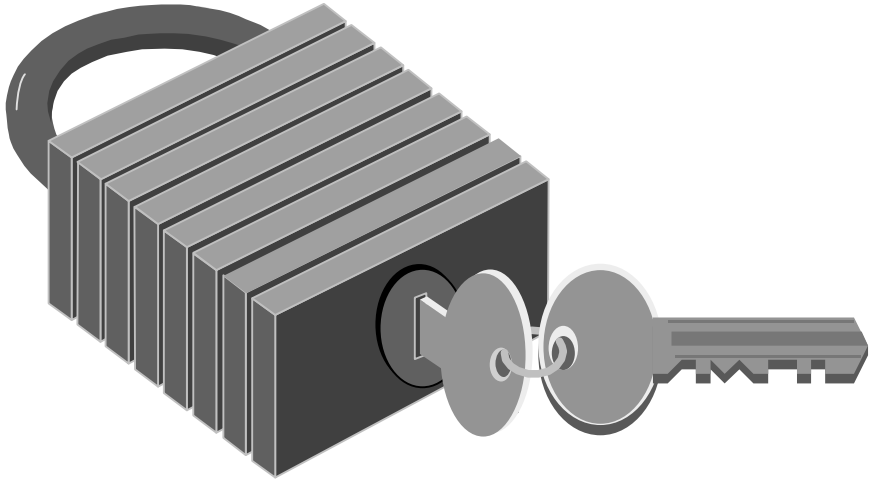
RSA

- Ron Rivest, Adi Shamir a Len Adleman (1977)
- Založen na neschopnosti lidí faktorizovat velká čísla
- Asymetrické šifrování



RSA

- V roce 1997 byl uveřejněn článek Jamese Ellise z britské CESG (Communications -- Electronics Security Group), nazvaný "The history of Non-Secret Encryption" , ve kterém jeho autor popisuje, jak princip asymetrické kryptografie (jím nazývaný jako Non-Secret Encryption, NSE) objevil už v roce 1970. Dále uvádí, že speciální variantu RSA objevil jeho kolega Clifford Cocks v roce 1973.



RSA (Algoritmus RSA)

I. Zvolíme abecedu A.

II. Text převedeme do číselné formy a rozdělíme na bloky stejné délky. Číselné vyjádření konkrétního bloku označíme x.

III. Zvolme N, součin dvou hodně velkých prvočísel (500 místných), tedy N = p*q. Musí platit 1<=x<N.

IV. Zvolíme si tzv. šifrovací exponent s tak, aby byl nesoudělný s funkcí f(N), respektive aby d(s,f(N)) = d(s,(p-1)*(q-1)) = 1, kde d(a,b) je největší společný dělitel.

V. Každý oznámí dvojici (N,s).

VI. Dále najdeme číslo t takové, že t*s = 1 mod f(N), resp. t*s = 1 mod (p-1)(q-1).

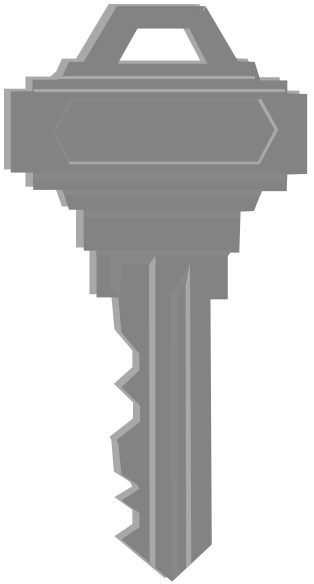
VII. Šifrujeme y = x^s mod N a dešifrujeme x = y^t mod N

RSA (Využití, bezpečnost, problémy)

- PGP
- není znám rychlý algoritmus na faktorizaci čísla N
- není dokázáno, že neexistuje
- nebylo ani dokázáno, že je nutno rozdrtit šifru pomocí modulární aritmetiky
- možná existuje algoritmus, který rozluští zašifrovaný text jinak
- najít dostatečně velká prvočísla **p** a **q** je pomalé - hledají se prvočísla s velmi velkou pravděpodobností

PGP

- Pretty Good Privacy, Phil Zimmermann
- aktuální verze PGP 8.0
- verze 2.x a 5.x při použití RSA:
  - RSA (asym, podpis)
  - IDEA (sym)
  - MD5 (hash)
- při použití DH/DSS:
  - Diffie-Hellman (El Gamalova varianta, asym)
  - IDEA n. 3DES n. CAST (sym)
  - DHH - Digital Signature Standard (asym při podpisu)
  - SHA-1 (hash)



PGP (Klíč)

- **ID** - binární číslo, jednoznačná identifikace, např. 0x59159CF1
- **User ID** - identifikace osoby (skupiny osob), které klíč patří; může být více
- **Signature** - podpis jiným klíčem, vyjádření jistoty jiné osoby, že klíč patří skutečně této osobě; libovolné množství; podepisují se jednotlivá User ID
- **Photo** - od verze 6.0 lze do klíčů vkládat fotografie ve formátech JPEG a BMP
- **Data** - samotný klíč, obsah závisí na typu klíče

PGP (Klíč)

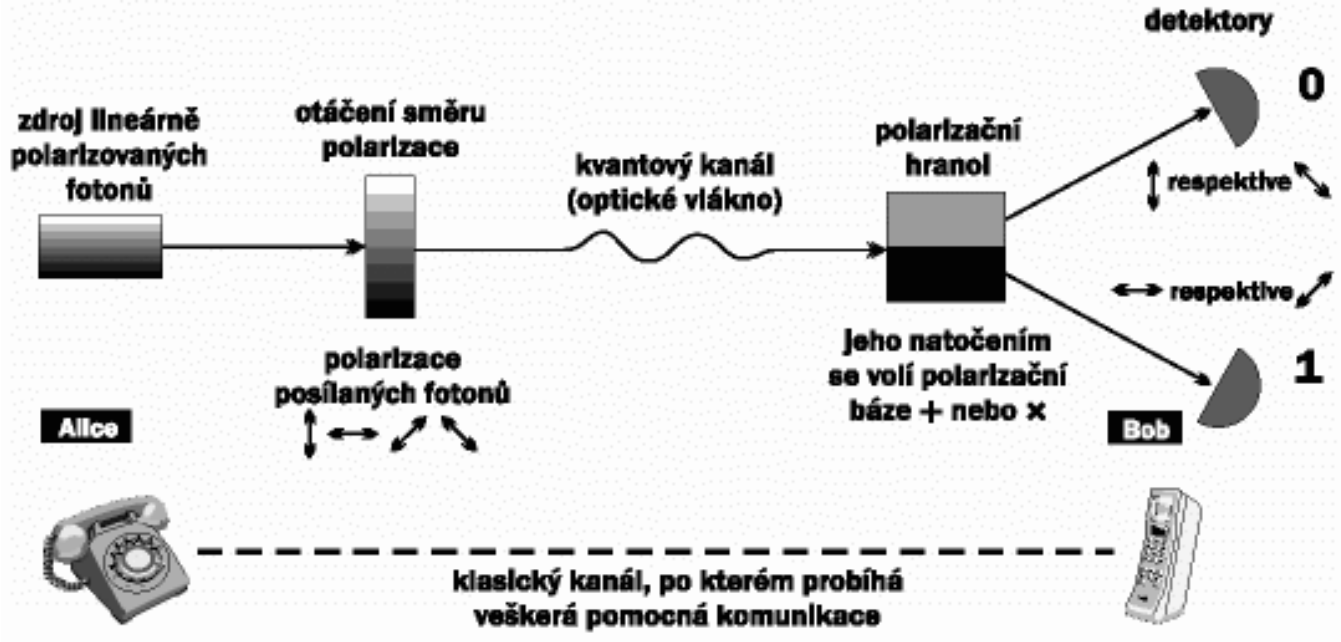
Public Key Server -- Get ``0x1A4FFA0E ''

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: 5.0
Comment: PGP Key Server 0.9.4

mQGiBDot4qsRBADJ5iQVTXCNdbqfPoZpNLkH/MfYSj8Z5MXb7XsEcgzadsQB3yUa
Da6iwv9bt8SgxKl+tpEIDboWuPMItmS8dVGhISoqn78Fria1e97tcwJF8Z+4NrcI
ru1uVr/g6AIpOt77k1lgjdCa/c/CmrguDOJZFAOJfWg55B+sZ3maFTOV6wCg/9jw
BIFOFP/vgM6tlRwnZOVp5RUEAJb1mfNLP9RzNHiLC4X/3BJc15sUUgnAHiTCBSTw
NSaI3CIdZBiBC5+HHU9I2QPmJRDd+ni0aCI4yX31/BDmk4dJ2E/NQ/PioJSySEkz
u167mfrTpjC2UBWGXrOZUGpu+7jjBJQFdZgtEOQHHBQkXQ5XSbfRZ1N16wQpQm6U
uYmCA/9BtU9ib7liRLXqizPgBxkKoHGqBQNhMHRPuM72PhQPk+hDzUK1ttw/wEnk
sICAaU8/zJLRCekfz4zEa5WJM3j1hFGCYo4O1PRZe2GD7wYwNB1WkqPMRpH9T4qb
Ok29YqzbutjEri3rG3tHTUPAbjI8NEN/zsEcpOj1QeKtswDe2bQdT25k+GVqIE5v
duFrIDxub3ZhaOBhZG9yZS5jej6JAFQEEBECABQFAjot4qsFCQHhM4AECwMCAQIZ
AQAKCRBZ2uQaGk/6DlAKAJ4OrDqXYEhKGk1o7toHbQZZoOd46ACgyp4D+hUR8T6Y
9POwkuhUOIJz8xu5AgOEOi3iqxAIAPZCV7cIfwgXcqK61q1C8wXo+VMROU+28W65
Szgg2gGnVqMU6Y9AVfPQB8bLQ6mUrfdMZIZJ+AyDvWXpF9ShO1D49Vlf3HZSTzO9
jdvOmeFXklnN/biudE/F/Ha8g8VHMGHOfMlm/xX5u/2RXscBqtNbno2gpXI61Brw
vOYAWCvl9Ij9WE5J28OgtJ3kkQc2azNsOA1FHQ98iLMcfFstjvbzySPAQ/ClWxiN
jrtVjLhdONMO/XwXVOOjHRhs3jMhLLUq/zzhsSlAGBGNfISnCnLWhsQDGcgHKXrK
lQzZlp+rOApQmwJGOwg9ZqRdQZ+cfL2JSyIZJrqrol7DVekyCzsAAgIIAJSLWwm5
QGyQe7XKdg626M+5sPgt78OWpOLDDvMZlK4nI16kTO1PX9/biTa7EczjCuCVFRIA
zFmMJDw+fdAprnYUek6fRYoGyHxY87fgZEImYsBkGFPK3X/gxRLWSZ/QlpR78F42
FA6ZN46+5gB/QWKGIBB346Zcin758khVFRL+UyPTDKWEBEJ893714uOTALDhdP4Q
ot1BkCIFyIylkZJ/7KefoyOLt7SP4k6B+vydBjIAWeiQnT4yujmSH9mWKsAORO6I
z9sCY5OYJGg6gADI/GSlDEK9Fm94GAU+zkUZOOCw5ejUHsdEW+AvCxtC1QVVxvE5
wyFhnJZI73olWi6JAEwEGBECAAwFAjot4qsFCQHhM4AACgkQWdrkGhpP+g6nNQCd
EeFDyATzrHiIYNUKajjx4skgvEUAoKRzOvh/zvzNyMBZbRNugTJrZ+SX
=tcTf
-----END PGP PUBLIC KEY BLOCK-----
```

Kvantová kryptografie

- **Kvantová kryptografie řeší problém distribuce kryptografického klíče. Neumí sice odposlechu zabránit, ale umožňuje spolehlivě zjistit, zda k odposlechu došlo. A to v případě přenosu klíče úplně stačí.**



Zdroje

- www.google.com